

NetDiligence[®]

2018
CYBER
CLAIMS
STUDY

2019 Spotlight

RETAIL

SPONSORED BY



Introduction

NetDiligence® is pleased to release this spotlight report on cyber claims within the Retail sector. From our dataset of over 1,200 claims provided by our insurance partners, we have classified and analyzed 124 claims from the Retail sector. These claims provide insight into losses sustained from cyber events during the five-year period 2013–2017.

The Retail sector is a significant part of the American economy. According to a report from the National Retail Federation¹, the Retail sector:

- Consists of 3.8 million establishments, of which 99% employ fewer than 50 people
- Contributes \$1.2 trillion dollars per year directly to US GDP
- Provides 29 million jobs and \$822.5 billion per year in salaries and wages
- Indirectly supports 13 million additional jobs and indirectly contributes an additional \$1.4 trillion to US GDP

Because a large majority of people purchase goods and services using payment cards, and because the attack surface presented by both brick-and-mortar retail and e-commerce organizations is vast and full of vulnerabilities, it should come as no surprise that malicious actors target the Retail sector to steal credit and debit card information. For these reasons, we have seen more claims involving payment card data and PCI issues in Retail than in other sectors.

As you review the findings in this report, please keep in mind that most of the data breach claims in this study involved smaller organizations (SMEs). Please note that:

- As a result, our median and average costs may be lower than the breach costs reported in more general studies.
- The dataset included several “mega-breach” events, all of which occurred prior to 2017. That may explain why many of the 2017 totals are much lower than the five-year numbers.

¹ *The Economic Impact of the US Retail Industry*, National Retail Federation

Findings

Breach Costs - Overall

- Average Breach Costs for Retail claims were \$1.2M (five-year) and \$178K (2017). Median overall Breach costs were \$94K (five-year) and \$80K (2017).
- Criminal and malicious activity accounted for 88% (five-year) and 91% (2017) of claims. The average Breach Costs for these claims were \$1.3M (five-year) and \$169K (2017). For non-criminal claims, the average Breach costs were \$276K (five-year) and \$263K (2017).
- For the five-year period, 65% of events exposed records and 35% did not. The average Breach Costs were dramatically different: \$1.6M for events that exposed records and \$352K for recordless events.
- The average number of records exposed was 4.6M (five-year); the median was 12K. The largest number of records exposed was >100M.
- Per-record costs ranged from less than one-tenth of a cent to more than \$6.7K. The average per-record cost was \$173; the median was \$8.56.

Crisis (Post-breach) Services Costs

- Average Total Crisis Services costs were \$373K (five-year) and \$169K (2017).
- For the individual categories of Crisis Services, the average costs were:
 - Forensics: \$291K (five-year) and \$136K (2017)
 - Legal Guidance/Breach Coach®: \$107K (five-year) and \$33K (2017)
 - Credit/ID Monitoring: \$78K (five-year) and \$20K (2017)
 - Notification: \$72K (five-year) and \$18K (2017)
- Average Legal Defense costs were \$329K (five-year) and \$55K (2017).
- Average Legal Settlement costs were \$388K (five-year) and \$7K (2017).
- Average Regulatory Defense costs were \$84K (five-year).
- Average Regulatory Fines were \$45K (five-year).
- Average PCI Fines were \$1.2M (five-year).
- Average Lost Business Income costs were \$80K (five-year) and \$102K (2017).
- Average Recovery Expense costs were \$57K (five-year and 2017).
- Average Breach Costs (five-year) for retail organizations with <\$2B in revenues were significantly lower than for ones with >\$2B in revenues: \$498K vs \$4.95M.

Discussion

Cause of Loss

Hacking (30%) and Malware/Virus (27%) were the most common causes of loss, accounting for 57% of claims for the five-year period and 47% in 2017. These two causes of loss accounted for 94% of Breach Costs for the five-year period and 68% in 2017.

Third Party Legal actions² (18% of claims for the five-year period; 9% in 2017), and Ransomware (7% of claims for the five-year period; 19% in 2017) round out the top four causes of loss. Average Breach Costs were:

Average Breach Costs Ranked by Percentage of Claims	Five-Year	2017
Hacking	1,537,815	167,495
Malware/Virus	2,419,353	401,012
Third Party/Legal Actions	254,789	106,438
Ransomware	61,912	63,138

Of note: Programming errors, though infrequent (2% of claims over five years), were costly, with an average Breach Cost of \$394K.

The four most expensive causes of loss— based on average Crisis Services Costs for the five-year period— were due to Hacking, Malware/Virus, Trademark/Copyright Infringement and Programming Errors.

Average Crisis Services	Five-Year	2017
Hacking	569,906	98,984
Malware/Virus	537,776	541,095
Trademark/Copyright Infringement	468,066	468,066
Programming Errors	354,000	No claims

² This category includes events that generated third-party legal action costs and/or CPP investigation expense.

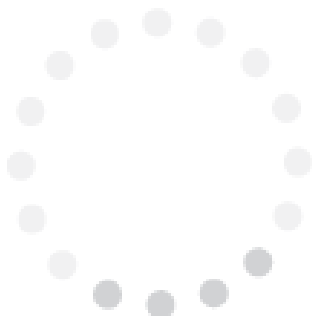
Types of Data

Data of all types was compromised in the Retail sector. PCI claims were most frequent (53%), followed by PII (11%) and Files – Critical³ (11%). The following three tables present the five-year summary statistics for PCI, PII, and Files – Critical data.

Retail PCI 2013 - 2017	Claims	Min	Average	Median	Max
Records	54	<100	\$5.8M	16.5K	>100M
Breach Cost	66	\$10K	\$1.96M	\$132K	>\$16M
Per-record Breach Cost	54	<0.001	\$69.58	\$5.91	\$1,604
Total Crisis Services Cost	50	\$5K	\$603K	\$81K	>\$4.8M

Retail PII 2013 - 2017	Claims	Min	Average	Median	Max
Records	8	300	33.5K	1,625	249K
Breach Cost	12	\$9K	\$170K	\$63K	\$678K
Per-record Breach Cost	8	\$2.72	\$141.25	\$86.02	\$661.18
Total Crisis Services Cost	11	\$2K	\$136K	\$75K	\$1.5M

Retail Files – Critical 2013 - 2017	Claims	Min	Average	Median	Max
Records	N/A				
Breach Cost	14	\$11K	\$155K	\$69K	\$700K
Per-record Breach Cost	N/A				
Total Crisis Services Cost	9	<\$500	\$96K	\$30K	\$680K



³ Most Ransomware, DDoS, Wire Transfer/Banking Fraud, and Network Outage claims do not expose records. "Files – Critical" is a Type of Data introduced in the 2018 NetDiligence® Cyber Claims Study to characterize these kinds of claims.

Other Significant Findings

PCI Fines

In the dataset, 53% of Retail sector claims exposed PCI/Credit Card data, however only 6% of claims involved a PCI fine. Many claims did not meet exposed card account thresholds⁴ as outlined in the Card Brand contracts, while other claims remained open. The PCI Council's time from breach to rendering an actual assessment is eighteen months to three years after a breach.

The analysis showed that when a fine occurred, it tended to be large, as the five-year table below shows:

PCI Fines	Claims	Min	Average	Median	Max
2013 - 2017	7	\$56K	\$1.2M	\$235K	\$6.9M

POS-Related

Point of Sale (POS) systems provide an attractive and lucrative attack vector for malicious actors. Each brick-and-mortar retail establishment has one or (many) more of these devices at each location. While there are tens of millions of POS devices, there are just a handful of POS hardware and software suppliers. This means that an exploit for one vendor's platform, say IBM or Micros, opens the door to hundreds and even thousands of targets.

Approximately 11% of the claims in the Retail sector dataset involved compromised POS devices. Following are the summary statistics:

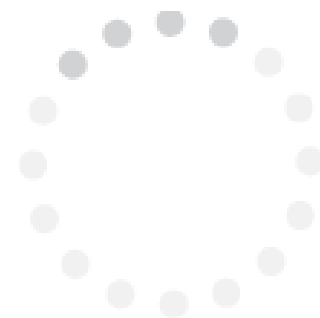
POS-Related 2013 - 2017	Claims	Min	Average	Median	Max
Records	14	14K	12.3M	1.2M	>100M
Breach Cost	19	\$17K	\$3.4M	\$500K	>\$16M
Per-record Breach Cost	14	\$0.02	\$5.51	\$4.96	\$15.32
Total Crisis Services Cost	15	\$7K	\$1.25M	\$186K	\$3.95M

⁴ VISA and Mastercard stipulate that a minimum number of unique card accounts must be compromised before certain cost recovery provisions come into effect. Prior to January 1, 2016, this threshold was 5,000 accounts. After January 1, 2016, each of these Card Brands raised the threshold to 30,000 card accounts.

Common Point of Purchase (CPP) Investigations

The Card Brands (VISA, Mastercard, American Express, Discover, etc.) have a unique view into all payment card traffic. When a Card Brand detects a pattern of fraud that can be tied to a single merchant, it will often open a CPP investigation. The forensics cost of this investigation must be borne by the merchant, who is required to utilize the services of a Card Brand-approved PCI Forensics Investigator (PFI). Often, these investigations fail to find any fault or evidence of a breach on the part of the merchant. Unfortunately, in these cases the merchant and its insurer are still liable for the cost of investigation.

Here are the summary statistics for cyber events that also involved a CPP investigation:



CPP Investigations 2013 - 2017	Claims	Min	Average	Median	Max
Records	8	14K	229K	23K	1.25M
Breach Cost	9	\$24K	\$1.1M	\$82K	\$8.9M
Per-record Breach Cost	8	\$0.82	\$4.91	\$4.02	\$13.64
Total Crisis Services Cost	9	\$14K	\$492K	\$69K	\$3.9M
CPP Claim Forensics	7	\$8K	\$317K	\$30K	\$2.1M

E-Commerce and Web Platforms

Approximately 8% of the claims from 2013-2017 involved the compromise of websites and e-commerce platforms, all by hacking and malware/virus attacks. PCI/credit card data was compromised in 60% of these events; Non-Card Financial, PII, and Files – Non-Critical were involved in the other 40%.

E-commerce and web platforms, if not well designed and coded with cybersecurity in mind, are especially vulnerable to exploit. Most web applications utilize software components and libraries from multiple sources, and sometimes multiple sources within multiple sources. There is enormous pressure on software developers to get applications up and running, and secure cyber coding is sometimes the last thing developers want to hear about.

These are the summary statistics for websites and e-commerce:

Web & E-Commerce 2013 - 2017	Claims	Min	Average	Median	Max
Records	6	\$300K	8.6K	4.4K	30K
Breach Cost	10	\$10K	\$148K	\$91K	\$716K
Per-record Breach Cost	6	\$7.92	\$40.13	\$22.53	\$117.22
Total Crisis Services Cost	10	<\$5K	\$137K	\$66K	\$696K

Conclusion

Eleven years ago, the Payment Card Industry Council issued the first PCI standards. These standards identified specific steps in network security and secure application development and deployment that organizations had to implement to achieve PCI compliance and to improve the security of payment card systems. Since then, the PCI Council has issued several additional standards and updates to the original PCI-DSS, most recently in early 2019.

Securing payment card processing environments and maintaining PCI compliance is difficult. Many retailers must patch vulnerabilities in thousands of applications on their networks. Effective assessments of third party and purchased applications, their connectivity, and the integration of these applications with existing security systems continues to be a central concern. The work to quantify the actual risk to the business while increasing the operational efficiency of mitigating these risks is challenging.

An increasing number of merchants and payment processors have implemented end-to-end encryption technology in their payment processing networks. It is also likely that widespread adherence to the PCI-DSS framework has had a positive impact on cyber losses in the Retail sector.

It is too early to know whether the lower numbers in 2017 represent a true downward trend or just an anomaly in our convenience sampling. We are in the process of collecting and analyzing new data for the 2019 NetDiligence® Cyber Claims Study. This report will include additional data for 2016 and 2017, and new data for 2018. Please watch for this important publication in the fourth quarter of 2019.

A Note on Methodology

Our data collection, analysis, and reporting methodology are described in detail in the full 2018 NetDiligence® Cyber Claims Study.

Contact Us

For more information about NetDiligence® or any of our service offerings, please visit us at [NetDiligence.com](https://www.netdiligence.com), email us at management@netdiligence.com, or call us at 610.525.6383.

